(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 September 2003 (25.09.2003)

PCT

(10) International Publication Number
WO 03/079606 A1

(51) International Patent Classification[7]: H04L 9/00, G06K 9/62, H04L 9/32, H04B 1/66

(21) International Application Number: PCT/US03/07776

(22) International Filing Date: 12 March 2003 (12.03.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/100,233 13 March 2002 (13.03.2002) US

(71) Applicant *(for all designated States except US)*: **DIGIMARC CORPORATION** [US/US]; Suite 250, 19801 S.W. 72nd Avenue, Tualatin, OR 97062 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **LOFGREN, Neil, E.** [US/US]; 163 Palos Verdes, White Salmon, WA 98672 (US). **RHOADS, Geoffrey, B.** [US/US]; 2961 S.W. Turner Road, West Linn, OR 97068 (US).

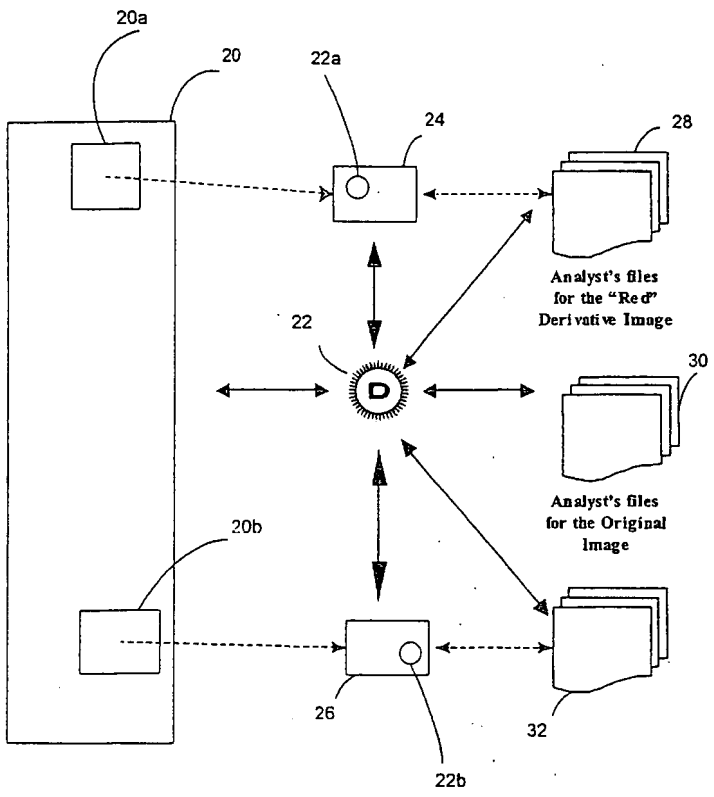
(74) Agent: **CONWELL, William, Y.**; Digimarc Corporation, Suite 250, 19801 S.W. 72nd Avenue, Tualatin, OR 97062 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),

[Continued on next page]

(54) Title: IMAGE MANAGEMENT SYSTEM AND METHODS USING DIGITAL WATERMARKS



(57) Abstract: Digital watermarking technology is used as an image management system(30). Images are identified by digital watermarks (22a and 22b). The images are stored so as to be indexed according to their unique identifiers (22). In the preferred embodiment, related images are grouped into a set of images through a common watermark identifier (28). A particular image within the set of images is identified through a hash of the particular image (22).

WO 03/079606 A1

European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:
— *with international search report*

IMAGE MANAGEMENT SYSTEM AND METHODS USING DIGITAL WATERMARKS

Related Application Data

[0001] This application claims the benefit of U.S. Patent Application No. 10/100,233, filed March 13, 2002. This application is also related to U.S. Patent Application No. 09/858,336, filed May 15, 2001, titled "Image Management System and Methods Using Digital Watermarks." This patent application also claims the benefit of U.S. Provisional Application No. 60/284,776, filed April 18, 2001, titled "Using Embedded Identifiers with Images."

[0002] This patent application is also related to assignee's U.S. Patent Application Nos. 09/833,013, titled "Digitally Watermarked Maps and Signs and Related Navigational Tools," filed April 10, 2001, and 09/800,093, filed March 5, 2001, titled "Geo-Referencing of Aerial Imagery Using Embedded Image Identifiers and Cross-Referenced Data Sets," and U.S. Provisional Patent Application No. 60/284,163, filed April 16, 2001, titled "Watermark Systems and Methods."

Field of the Invention

[0003] The present invention relates to image management and processing, and is particularly illustrated in the context of a satellite and other aerial imagery management system.

Background and Summary of the Invention

[0004] Aerial imagery has vastly improved since the Wright brothers first took to the sky. Indeed, there have been many improvements in the photography and digital imaging fields.

[0005] While the earliest aerial imagery relied on conventional film and optics technology, a variety of electronic sensors are now more commonly used. Some collect image data corresponding to specific visible, UV or IR frequency spectra (e.g., the MultiSpectral Scanner and Thematic Mapper used by the Landsat satellites). Others

use wide band sensors. Still others use radar or laser systems (sometimes stereo) to sense topological features in 3 dimensions. Some satellites even collect ribbon imagery (e.g., a raster-like, 1-demensional terrestrial representation, which is pieced together with other such adjacent ribbons).

[0006] The quality of the imagery has also constantly improved. Some satellite systems are now capable of acquiring image and topological data having a resolution of less than a meter. Aircraft imagery, collected from lower altitudes, provides still greater resolution.

[0007] A vast amount of aerial imagery is constantly being generated and collected. Management of the resulting large data sets is a growing problem. In today's digital world, images are routinely manipulated, even on home computers. Management of resulting image ancestry, image derivatives and related metadata is increasingly difficult.

[0008] According to one aspect of the present invention, a digital watermark-based image management system helps solve these and other problems. A digital watermark is ideally employed as link or bridge to group a related family of images. An image family can be associated in a database (or other data structure) via a parent's digital watermark identifier. Individual images within the image family are identified by a unique image hash (or fingerprint).

[0009] Digital watermarking is a form of steganography that encompasses a great variety of techniques by which plural bits of digital data are hidden in some other object without leaving human-apparent evidence of alteration.

[0010] Digital watermarking may be used to modify media content to embed a message or machine-readable code into the content. The content may be modified such that the embedded code is imperceptible or nearly imperceptible to the user, yet may be detected through an automated detection process.

[0011] Most commonly, digital watermarking is applied to media such as images, audio signals, and video signals. However, it may also be applied to other types of data, including documents (e.g., through line, word or character shifting, through texturing, graphics, or backgrounds, etc.), software, multi-dimensional graphics models, and surface textures of objects.

[0012] The assignee's U.S. Patent No. 6,122,403, and co-pending U.S. Patent Application No. 09/503,881, detail suitable digital watermarking techniques in which values of pixels, e.g., in a 100 x 100 pixel patch, can be slightly altered so as to convey a plural-bit payload, without impairing use of the pixel data for its intended purpose. The payload may be on the order of 2 – 256 bits, depending on the particular form of encoding (e.g., convolution, turbo, or BCH coding can be employed to provide some error-correcting capability), and the number of bits per pixel. Larger payloads can be conveyed through larger image patches. (Larger payloads can also be conveyed by encoding the information in a less robust fashion, or by making the encoding more relatively visible.). The watermark payload can convey an image identifier, and may convey other metadata as well. In some embodiments, the component image files are tagged both by digital watermark identifiers and also by conventional out-of-band techniques, such as header data, thereby affording data redundancy. Of course, there are many watermarking techniques known to those skilled in the art, and such may be suitably interchanged with the present invention.

[0013] Digital watermarking systems typically have two primary components: an embedding component that embeds the watermark in the media content, and a reading component that detects and reads the embedded watermark. The embedding component embeds a watermark pattern by altering data samples of the media content. The reading component analyzes content to detect whether a watermark pattern is present. In applications where the watermark encodes information, the reading component extracts this information from the detected watermark. Commonly assigned U.S Application No. 09/503,881 discloses various encoding and decoding techniques. United States Patent No. 5,862,260 discloses still others.

[0014] Watermarking may be performed in stages, at different times. For example, a unique identifier can be watermarked into an image relatively early in the process, and other information (such as finely geo-referenced latitude/longitude) can be watermarked later. A single watermark can be used, with different payload bits written at different times. (In watermark systems employing pseudo-random data or noise (PN), e.g., to randomize some aspect of the payload's encoding, the same PN data can be used at both times, with different payload bits encoded at the different times.).

[0015] Alternatively, different watermarks can be applied to convey different data. The watermarks can be of the same general type (e.g., PN based, but using different PN data). Or different forms of watermark can be used (e.g., one that encodes by adding an overlay signal to a representation of the image in the pixel domain, another that encodes by slightly altering DCT coefficients corresponding to the image in a spatial frequency domain, and another that encodes by slightly altering wavelet coefficients corresponding to the image. Of course, other watermarking techniques may be used as suitable replacements for those discussed above.).

[0016] In some multiple-watermarking approaches, a first watermark is applied before a satellite image is segmented into patches. A later watermark can be applied after segmentation. (The former watermark is typically designed so as to be detectable from even small excerpts of the original image.)

[0017] A watermark can even be applied by an imaging instrument. In some embodiments, the image is acquired through an LCD optical shutter, or other programmable optical device, that imparts an inconspicuous patterning to the image as it is captured. (One particular optical technique for watermark encoding is detailed in U.S. Patent No. 5,930,369.). Or the watermarking can be effected by systems in a satellite (or other aerial platform) that process the acquired data prior to transmission to a ground station. In some systems, the image data is compressed for transmission – discarding information that is not important. The compression algorithm can discard information in a manner calculated so that the remaining data is thereby encoded with a watermark.

[0018] A ground station receiving the satellite transmission can likewise apply a watermark to the image data. So can each subsequent system through which the data passes, if desired.

[0019] Preferably, such watermarking processes are secure and cannot be replicated by unauthorized individuals.

[0020] The foregoing and additional features and advantages of the present invention will be even more readily apparent from the following detailed description with reference to the following figures.

Brief Description of the Drawings

[0021] Fig. 1 is a functional block diagram illustrating image capture and a digital watermarking process.

[0022] Fig. 2 illustrates components of an image management system.

[0023] Fig. 3 illustrates associating related images and information with a digital watermark identifier.

[0024] Fig. 4 is a functional block diagram illustrating gatekeepers in a network.

[0025] Figs. 5 and 6 are flow diagrams illustrating gate-keeping methods and processes.

[0026] Figs. 7 and 8 variously illustrate a digital watermark identifier and an image hash used to identify and image family and images and metadata with the image family.

Detailed Description

[0027] For expository convenience, the following discussion focuses on satellite and other aerial "imagery" to illustrate the principles of the invention. The principles of the invention, however, are equally applicable to other forms of imagery, including non-aerial imagery. Accordingly, the term "image" should be used to encompass other data sets, and the term "pixel" should be construed to encompass component data from such other data sets. The term "image" should also be construed to include both digital and analog data sets.

Watermarking Images

[0028] With reference to Fig. 1, an image 10 is captured from an aerial platform 11, such as an aircraft, satellite, balloon, unmanned aircraft, etc. The image 10 is communicated to a receiving or ground station 12. (In some instances, the image signal may be relayed through various aerial and/or other ground stations before reaching ground station 12.). Ground station 12 preferably includes a digital watermark embedder 12a, which embeds a digital watermark within the image 10, to produce a digitally watermarked image 13.

[0029] A digital watermark is typically embedded in a digital representation of the image 10. Although not required, the digital watermark preferably survives transformation to various analog representations (e.g., printing) as well. The digital watermark includes a watermark identifier (ID). In a first embodiment, each image is digitally watermarked to include a unique watermark ID. The ID typically includes plural-bit data, e.g., in the range of 2-256 bits. In one implementation of this first embodiment, a digital watermark (and identifier) is redundantly embedded within an image to improve robustness. For example, an image is divided into tiles or sections, and each tile or section is embedded with the digital watermark (and ID). Alternatively, a subset of the sections are embedded. Such techniques help to ensure the robustness of a watermark, particularly when an image is to be manipulated (e.g., clipped, cut-and-pasted, resized or scaled, rotated, etc.).

[0030] Digitally watermarked image 13 is stored in a database 14. (A watermarked image can be directly communicated to database 14, transferred via a storage medium and/or otherwise relayed to database 14.). Database 14 preferably manages images and/or related data. Database software, e.g., such as provided by Microsoft, Oracle, Sun Microsystems, etc., can be executed by a computer or server to help maintain database 14. Of course, database 14 can be maintained by a ground station 12 system, or can be maintained in a remotely located network. In one implementation, database 14 communicates with a network, such as a LAN, WAN, dedicated network, wireless network, private network, etc. In some implementations, database 14 includes a plurality of databases. In such an implementation, at least one database maintains image data, while at least a second database maintains related image information (e.g., metadata, related files, comments, file history, edit history, and/or security clearance information, etc.). Here, metadata is broadly defined to include a variety of information such as creation data, geo-location information, ancestry data, security information, access levels, copyright information, security classifications, usage rights, and/or file history, etc.

[0031] Image 13 and/or any related metadata is preferably stored and indexed according to watermark IDs. For example, a watermark ID provides a thread by which images and related information are grouped, stored and/or indexed.

[0032] Optionally, original image data is communicated to a second database 15. Database 15 can be used to maintain original image 10 and/or an original watermarked image 13. (The dashed lines in Fig. 1 represent this optional embodiment.).

Image and Derivative Image Management Using Digital Watermarks

[0033] A problem faced by image management systems is how to efficiently manage an image's ancestry and related metadata. Normal image processing (e.g., scaling, cropping, rotating, clipping, resizing, cut-and-pasting image blocks, editing, annotating,

and/or marking, etc.) of an "original" image results in a "derivative" image. In conventional systems, derivative images frequently retain minimal, if any, related metadata. The metadata, such as that stored in header or footer files, is easily separable from derivative images. Separation results in a significant loss of information, particularly for a derivative image. One conventional solution is to manually record an image identifier as an image moves through an exploitation (or derivative) process. This manual recording process is labor intensive and cumbersome at best.

[0034] A better solution, as disclosed in this application, is to place a unique digital watermark ID within an image to enable database linking and indexing. Metadata contained within the database can be then associated with a specific image, or with a family of images, via the unique watermark ID. With reference to Fig. 2, a user terminal 18 retrieves a digitally watermarked image 001 from database 14. User terminal 18 preferably includes a processor, memory and suitable software instructions to facilitate digital watermark detection and/or embedding. The user terminal 18 will preferably include an operating system, such as Windows, Windows NT, Linux, etc., and image-handling (and editing) software. Suitable image-handling software can be obtained from Microsoft, Adobe, SRI and Erdas, among others. Preferably, both the watermark detecting software and the image-handling software are compatible with various types of image formats, such as bit-maps, JPEG files, TIF files, etc. (However, such compatibility is not required.).

[0035] Digital watermark detection software executing in user terminal 18 analyzes image 001. The watermark detection software can be called by the imaging software, may operate as a plug-in, or may be even integrated with the image-handling software, operating system, or other software module. The watermark detection software extracts the unique watermark identifier (e.g., ID-1) embedded within image 001. Having obtained the identifier (ID-1), the user terminal 18 can optionally communicate with database 14 to retrieve related information, such as metadata, files, and related images. For example, the watermark ID-1 is used to interrogate database 14 to retrieve information regarding the geo-coordinates for the image, the time and date the image was taken, analyst comments, and/or analyst information, etc. Preferably, the

watermark ID-1 is used to index any derivative images, e.g., derivative 001. (In this case, derivative 001 is an image derived from image 001.).

[0036] In a preferred embodiment, since each image includes a unique identifier, derivative 001 includes a watermark identifier (e.g., ID-5) that is unique from the corresponding original image 001 (e.g., identifier ID-1). Derivative 001 and image 001 are associated (e.g., linked) together in database 14, via identifier ID-1 (and, optionally, via ID-5).

[0037] In some instances, user terminal 18 will create additional derivatives. Take for instance, an example when user terminal 18 enlarges the derivative 001 image, thus creating a new derivative image 001a. This new derivative image 001a is preferably uniquely identified with a digital watermark. A process of digitally watermarking a derivative image typically involves removing the original watermark from the derivative and replacing that original digital watermark with a new digital watermark having a unique identifier. Thus, upon creating derivative image 001a, the digital watermarking software removes the derivative 001 watermark (or at least a portion of the watermark, e.g., identifier ID-5) from the derivative 001 image. Assignees' U.S. application 09/503,881 discusses relevant digital watermarking techniques. Artisans know others still that may be suitably interchanged with the present invention. Derivative 001a is then embedded with a digital watermark having a unique identifier (e.g., ID-10). (In an alternative implementation, the original watermark is altered, e.g., by changing one or more message bits, to create the new unique identifier, instead of replacing the original watermark with a new watermark. In another embodiment, a second watermark is added to the derivative image to complement the first (or more) watermark, instead of replacing the first watermark. In this case, the first watermark identifies the original image, and the second watermark identifies the derivative.).

[0038] The watermark embedding software can determine an appropriate identifier in a number of ways. In one embodiment, the embedding software queries database 14 for an appropriate, or available, identifier. In another case, embedding software (or user terminal 18) is assigned a range of identifiers, and an identifier is chosen from the available range. In still another embodiment, the embedding software randomly or pseudo-randomly selects the identifier, or alters a portion of the original image identifier, e.g., 2-32 bits of the original watermark identifier.

[0039] An image and a watermark identifier are combined to produce a digitally watermarked image (or derivative image). As an optional feature, software provides an indicator to signal success or failure in the watermarking effort. For example, the software can analyze whether the watermark was embedded, and/or whether the image contains the same format and density as the original input image. Upon a failure, user terminal 18 re-embeds the digital watermark or aborts the process.

[0040] Derivative image 001a is stored in database 14. Related information can also be stored in database 14. (As discussed above, database 14 may include a plurality of databases. One such database may manage images, while another database manages related information. Preferably, however, the unique identifiers are used consistently between the plurality of databases to link related images, derivatives and any associated metadata.). Database 14 links derivative 001a with image 001, derivative 001 and any related information (e.g., metadata, comments, files, history, security, etc.). Accordingly, image ancestry and any related information is efficiently maintained.

[0041] Figure 3 is a diagram further illustrating linking images, derivatives and related information via watermark identifiers. An original image 20 is digitally watermarked with a unique identifier 22. A first derivative image 24 (e.g., perhaps an enlarged or cropped image corresponding with area 20a) and a second derivative 26 (e.g., corresponding to area 20b) are created. Each of the first derivative 24 and second derivative 26 are encoded with a unique watermark identifier 22a and 22b, respectively. The derivative identifiers 22a and 22b are associated with the identifier 22 in database 14. Such linking effectively groups image families together, permitting a user to gain

access to image ancestry. Similarly, related information can be linked via unique identifier 22. Returning to Fig. 3, related information 28 corresponding to first derivative 24 are linked to identifier 22. Files 30 corresponding to the original image 20, as well as files 32 for the second derivative 26, are likewise linked. Accordingly, entire image families (and related information) are efficiently maintained by linking via the unique identifier 22. Of course, files 28 and 30 optionally can be separately, and respectively, linked to derivatives 24 and 26, via the derivatives' unique identifiers 22a and 22b (e.g., as shown by the dashed lines in Fig. 3).

Digital Watermarks and Image Hashes

[0042] In a related embodiment, we use an image hash to uniquely identify a derivative image and a digital watermark to identify the image family, image family line or image parent. We define the term "hash" broadly herein. Most generally, a hash is an algorithm that converts a signal (e.g., image) into a lower number of bits. The term "hash" can also represent the output or result of such a hashing algorithm. Of course our hash definition is broad enough to include so-called image fingerprints. A hashing algorithm may be applied to the whole image or to a selected portion of an image (e.g., image block(s), high frequency components of an image, frequency-domain characteristics, perceptually relevant image characteristics, etc.) to create a hash. Some hashing algorithm examples include MD5, MD2, SHA and SHA1. See assignee's U.S. Patent Application No. 10/027,783, filed December 19, 2001 for a further discussion of hashing, digital signatures and fingerprinting techniques. Of course, there are many other conventional hashing algorithms and techniques that may be suitably interchanged with the hashing aspect of this embodiment of our present invention.

[0043] With reference to Fig. 7, a parent image 002 is digitally watermarked. The digital watermark includes an identifier (e.g., WM 002). The digital watermark is preferably robust, e.g., it survives signal processing such as scaling, rotation, cropping, editing, etc. Accordingly, a derivative image 002 "inherits" the digital watermark including the identifier WM 002. There are advantages inherent with this

implementation, such as the preservation of a persistent link (e.g., the WM 002 identifier) between derivative 002 and its parent image 002. However, used alone a solution of a persistent watermark identifier may not always be sufficient to distinguish the parent image 002 from the child derivative image 002 -- complicating a situation where information (or metadata) that is related to only the parent or to the derivative might not be relevant to the other.

[0044] We combine digital watermarking and fingerprinting to solve this problem. A digital watermark identifier is used to identify a family (or set) of images. Each family member preferably includes the same watermark identifier. We also determine an image hash (or fingerprint) for each image (including derivatives). These hashes are used to uniquely identify an image within the family or set of images. Any new derivatives that are encountered can be added to a database with a new hash to uniquely identify the derivative in that image family.

[0045] Consider Fig. 7 again. A hash 1 is computed for image 002. Hash 1 is associated with image 002, e.g., within the database image family defined (or identified) by WM 002, to uniquely identify image 002. Metadata that is uniquely associated with image 002 can be linked to image 002 via hash 1 (see Fig. 8). Derivative 002 is associated with the image 002 family since it includes the digital watermark identifier WM 002. A hash 2 is computed for derivative 002. This hash 2 uniquely identifies the derivative 002. Derivative images 002a, 003 and 003a are similarly associated with the WM 002 family via their embedded digital watermark identifier WM 002. Each of these derivative images 002a, 003 and 003a (and any related metadata) can be uniquely identified within the WM 002 family via image hashes 3, 4 and 5, respectively.

[0046] Once an image database is populated as discussed above, our image lookup process will typically involve two main steps: 1) after extracting a digital watermark

identifier from an image, the extracted identifier is used to locate in a database a corresponding image family, and then 2) after calculating a hash of the image, the calculated hash is used to match or otherwise identify an image from a hash(es) associated with the image family. (We note that the calculated hash is calculated using the same or related hashing algorithm that was used to calculate the original hash stored in the database. We also note that since the number of derivatives within an image family will be relatively smaller than the entire population of database images, a calculated hash can be matched with the "closest" comparable hash, and in at least one implementation of our present invention, need not be an exact match.). Thus, a digital watermark identifier provides a link to a family of images, while an image hash identifies a particular image within the family. Any image with the same watermark identifier preferably links to related family data (metadata, analysts notes, etc.) but image specific data is preferably registered against a particular hash, allowing the differentiation of derivatives from each other and their parent.

[0047] This inventive implementation has an added benefit of being able to verify whether a particular image is an original image. For example, an image hash can be associated with metadata, e.g., to indicate that "this image is a derivative," "this image is a derivative of image X," "here is a link to the parent," "here is a link to other derivatives," "here is information that was registered against this derivative," "this image is an original or parent" and/or "here is information that was registered against the parent," etc., etc.

[0048] We note that as an alternative implementation, we can configure our database and database interrogation routines to locate in the database an image via an image hash, instead of first identifying an image family through the digital watermark identifier. In such an implementation, however, we preferably use a digital watermark identifier to link to other, related images and metadata.

[0049] These implementations can reduce the number of unique identifiers required for a large image/derivative management system. As a further improvement, we can include an image hash as part of a unique image digital watermark identifier. For example, a first digital watermark payload field may include an image identifier and a second digital watermark identifier may include the hash. Or the hash may comprise the entire digital watermark identifier/payload.

Security and Rewritable Watermarks

[0050] In another embodiment, a digital watermark provides information related to a permission level or a security clearance level. Such information can be reflected in a unique identifier or in a payload message. Alternatively, the watermark identifier can be used to interrogate a database to retrieve related security level requirements. Such security information can be used to regulate access to images, files, metadata and related information. For example, only users (or user terminals) having a corresponding permission level or security clearance are allowed to access the corresponding image. Suitable software instructions can examine the permission level (or security clearance) to determine whether a user (or terminal) has the necessary clearance.

[0051] One aspect of the present invention is to employ "rewritable" watermarks. A rewritable watermark includes a watermark of which all or a portion of which may be changed. In a preferred embodiment, only a portion (e.g., a portion of the payload) of a watermark is rewritten to update permission levels, reflect derivative work, etc.

[0052] There are often situations where it is desirable to carry some form of security access indicator in an image, e.g., via a digital watermark. The security access indicator defines a level of security required to view, edit or comment with respect to an image. Access to the image is then controlled by appropriately enabled software, which extracts the indicator (or receives the indicator from a watermark decoder) and determines a security level needed to handle the image. In one embodiment, the indicator indicates defines a required level. If a user's security level is equal to or

greater than (e.g., as determined from a password, user terminal identifier, login, linked security clearance level, etc.) that carried in a security access indicator, then a user is allowed access to the image or data. In another embodiment, a security code may indicate that a particular user can view the image, but cannot edit or store comments regarding such.

[0053] Consider the following example. An image "A" is defined to include an "unclassified" security classification. Image A's watermark then includes a unique identifier and additional plural-bits set to a predetermined number, e.g., all set to zero (or to a predetermined number or pattern). These additional plural-bits define the unclassified security classification. An image "B" is a derivative of image A, and has a "secret" security classification encoded in the plural-bits. Before either image A or B is opened (or requested) the security level contained within the watermark is validated against the security level of the individual requesting access, and permission is only granted to those with adequate clearance. In one implementation, local software (e.g., executing on a user terminal) validates the security access by decoding the watermark, extracting the security bits, and comparing the security bits (or corresponding security level) with the security clearance of a user (or terminal). In another implementation, software running on a central server monitors and validates security access. Or in another implementation software associated with the database regulates the security access.

Application Interface

[0054] Application interface software, residing on a user terminal, helps to facilitate communication between image-handling software and database 14. The interface can be incorporated in such image-handling software, operate as a plug-in, be integrated with the operating system, or may even be called by certain operations (e.g., data retrieval, editing, saving, etc.). Preferably, the interface generates (or works in connection with) a graphical user interface (GUI) for a user. The GUI helps to facilitate user login, data retrieval, and image creation and saving. Creation is defined broadly to include any alteration to an existing image, or generation of a new image.

Initially, a user is requested to enter a password or pass code to interact with database 14. After a successful log in, user access is preferably regulated based on security clearance. In other embodiments, permission levels or payment schedules are used to regulate access. An image, and related metadata, files, etc., should only be accessible when security access is permitted. In one implementation, an image is selected from a directory, and the selected image is examined for watermarks. A watermark is extracted and security bits are determined. The security bits are validated against a corresponding security access allowed for the logged-on user. A user is permitted to access (e.g., retrieve, open, or edit) the image if she has an appropriate clearance. In an alternative arrangement, a database is queried to determine the security level required for all (or a subset of all) possible images in a directory or list. Only those images corresponding to the user's security clearance (or permission) are presented as options to open for the user. Even the names of the images can be screened from a user if her security clearance is insufficient.

[0055] The interface also facilitates communication in a normal image editing and creation processes. Preferably, the interface will be invoked as part of a saving process.

[0056] The creation process typically involves determining a new image identifier. As discussed above, there are many ways to determine an image identifier. In one case, the interface queries the database 14 to obtain a new image identifier. The retrieved image identifier is embedded in the newly created image as a portion of a digital watermark. The embedded image is then saved in database 14. Optionally, the database will signal that the save operation has been successfully completed. In the case of derivatives, the database is preferably updated to indicate that the new image identifier is related (or linked) to the identifier of an original image.

[0057] In one embodiment, the above-mentioned steps (e.g., creating, watermarking, and saving) are considered a transaction, e.g., where all of the steps must be carried out for the transaction to be complete.

Sentry

[0058] Another aspect of the present invention is a gatekeeper module. With reference to Figure 4, a gatekeeper (or "sentry") 42 (e.g., including 42a and 42b) resides on network terminals 40 and 44. Terminals 40 and 44 communicate, e.g., via a network, direct link, e-mail, etc. Sentry 42 monitors the flow of digital watermarked images and related information by extracting digital watermark identifiers or embedded security information from transmitted images. The sentry 42 can compare extracted information against user (or terminal) security clearance information. In one implementation, sentry is a software module, although sentry 42 may be incorporated into other software components (e.g., applications, operating system, etc.) of a network terminal 40 and 44. Sentry 42 monitors and controls the flow of images at various points in a network system. Such activity is logged (e.g., recorded, stored, etc.) in database 46. To monitor an image transmitted from user terminal 40 to user terminal 44, sentry 42a decodes an embedded watermark identifier from an image to be transferred (step S10, Fig. 5). The identifier, destination address, and optionally a date/time stamp are communicated to database 46 (step S12), where such information is recorded as a data record (or file, log, table, database entry, history, etc.) as in step S14. Preferably such transmission activity is associated with the unique identifier of the transferred image.

[0059] Sentry 42 is also gatekeeper in that it analyzes whether a user's security or permission level is sufficient to receive a watermarked image into or from a workstation (e.g., whether terminal 44 can receive the image transmitted from terminal 40). Sentry 42b preferably includes (or communicates with) watermark-decoding software, which extracts unique identifiers (and any security bits) from digitally watermarked images (step S20, Fig. 6). If the security level of an image is stored in a database, sentry 42b queries the database with the identifier to determine the required access level. Or if the watermark includes security bits, then sentry 42b determines an access level directly from extracted security bits. Sentry 42b determines whether the user's security clearance sufficiently corresponds with the received image's clearance requirements (step S22). If so, sentry 42b allows terminal 44 to receive and open the

subject image (step S24). If not, sentry 42b denies terminal 44 access to the image (step S26). In either case, sentry 42b preferably communicates such information to database 46 (step S28). For example, sentry 42b records whether the image is passed to terminal 44, or whether the image is denied. (As an optional function, sentry 42b notifies terminal 42 regarding the delivery status of the image.).

[0060] Preferably, sentry 42 does not performed the function of managing the relationship between images and their derivatives, as this is the function of the file save software associated with the image editing application. However, in one embodiment, sentry 42 is combined with an application interface.

[0061] Sentry 42 can be deployed in a number of ways. In one embodiment, sentry 42 is integrated (or stored, or connected) to a workstation or server in such a way that all image data must first pass through the sentry 42. In another embodiment, sentry 42 includes a separate hardware (or hardware/software) device inserted between a network (or network connection) and a user terminal. As such, sentry 42 decodes watermarks and intercepts passwords from image traffic before the user terminal receives the image, or directly after transmitting an image.

[0062] In another embodiment, e.g., in a TCP/IP environment, a sentry 42 is deployed as software within a TCP/IP stack in the user station or server. In yet another embodiment, a sentry is incorporated in (or called by) an image-handling program's open, save and close operations.

[0063] When used in connection with a database history or other record, sentry 42 provides efficient tracking and tracing. Since the history file reveals each use (and printing, transmission, etc.) of a watermarked image, the image can be efficiently tracked as it passes from terminal to terminal, or from database to terminal, etc.

Fragile Watermarks

[0064] Some images may include at least two watermarks. A first watermark includes a unique identifier, as discussed above. This identifier allows database inquires and association as discussed above. A second watermark can be applied prior to printing, faxing, etc. This second watermark preferably includes a so-called fragile watermark. That is, it is designed to be lost, or to degrade predictably, when the data set into which it is embedded is processed in some manner. (Fragile watermark technology is disclosed, e.g., in applications 09/234,780, 09/433,104, 09/498,223, 60/198,138, 09/562,516, 09/567,405, 09/625,577, 09/645,779, and 60/232,163.).

[0065] Once an image is printed, it then includes both the first and second watermarks. If the image is subsequently scanned back into a digital form, e.g., via a scanner, photocopier, web cam, digital camera, etc., the fragile watermark is corrupted (or lost) in a foreseeable manner. Printed copies can be tracked and traced accordingly. For example, a photocopied image is scanned into a digital form. The first watermark is used to identify the image and retrieve an image history (e.g., as created by a sentry or other logging method). Since the fragile watermark is lost (or predictably degraded) in the copy process, the photocopy is determined to be an unauthorized copy. The history log can be used to determine which user (or user terminal) printed the copy.

Conclusion

[0066] Watermarks can be applied to any data set (e.g., an image, map, picture, document, etc.) for forensic tracking purposes. This is particularly useful where several copies of the same data set are distributed through different channels (e.g., provided to different users). Each can be "serialized" with a different identifier, and a record can be kept of which numbered data set was provided to which distribution channel. Thereafter, if one of the data sets appears in an unexpected context, it can be tracked back to the distribution channel from which it originated.

[0067] In an alternative embodiment, with reference to Fig. 1, a digital watermark embedder is included in aerial platform 11. The aerial embedder embeds images (e.g., after or during capture) and relays such to ground station 12. In yet another embodiment, an image is digitally watermarked downstream from ground station 12, such as in a user terminal, or an embedder associated with the databases 14 and/or 15.

[0068] Although not belabored, artisans will understand that the systems described above can be implemented using a variety of hardware and software systems. One embodiment employs a computer or workstation with a large disk library, and capable database software (such as is available from Microsoft, Oracle, etc.). The watermarking and database operations can be performed in accordance with software instructions stored in the disk library or on other storage media, and executed by a processor in the computer as needed. (Alternatively, dedicated hardware, or programmable logic circuits, can be employed for such operations.). We note that while we have described our hashing and digital watermarking management implementation with reference to images, the present invention is not so limited. Indeed, we can similarly manage audio and video as well with our inventive techniques.

[0069] The various section headings in this application are provided for the reader's convenience and provide no substantive limitations. The features found in one section may be readily combined with those features in another section.

[0070] The particular combinations of elements and features in the above-detailed embodiments are exemplary only; the interchanging and substitution of these teachings with other teachings in this application and the above-mentioned patents/applications are also contemplated.

[0071] It should be appreciated that the present invention is not limited to managing satellite and other aerial imagery. Indeed, other imagery may be managed with the present invention. Also, the present invention encompasses a "non-secure" type of

system. In one such embodiment, watermark identifiers are used to link images and/or related information. A security or permission level is not required in such a system.

[0072] In view of the wide variety of embodiments to which the principles and features discussed above can be applied, it should be apparent that the detailed embodiments are illustrative only and should not be taken as limiting the scope of the invention. Rather, we claim as our invention all such modifications as may come within the scope and spirit of the following claims and equivalents thereof.

What is Claimed is:

1. A method of managing images in a database, wherein a first image includes a digital watermark comprising a first identifier embedded therein, said method comprising the steps of:

providing a first hash of the first image; and

uniquely identifying the first image in the database with the first hash of the first image.

2. The method according to claim 1, wherein a second image includes a digital watermark comprising the first identifier embedded therein, said method further comprising the step of:

in the database, associating the second image with the first image via the first digital watermark identifier.

3. The method according to claim 2, further comprising the steps of:

providing a first hash of the second image; and

in the database uniquely identifying the second image with the first hash of the second image.

4. The method according to claim 3, wherein the second image comprises a derivative of the first image.

5. A method according to claim 4, wherein related information is associated with at least the first image by the first hash of the first image.

6. The method according to claim 5, wherein the related information comprises at least one of user usage, creation time, transmission, printing, analyst notes, an audit trail, depicted geographic location, image capture time and image checkout.

7. The method according to claim 5, wherein the database comprises a plurality of databases.

8. The method according to claim 5, wherein the related information comprises at least one of metadata, location, date, permission level, security access levels, analyst comments, an audit trail, notes, files, and past usage information.

9. A method of managing a set of images, the set of images including a first image comprising a first identifier steganographically embedded therein in the form of a digital watermark and a second image comprising the first identifier steganographically embedded therein in the form of a digital watermark, said method comprising the steps of:

associating the first image with the set of images by the first identifier;

uniquely identifying the first image within the set of images with a hash of the first image;

associating the second image with the set of images by the first identifier; and

uniquely identifying the second image within the set of images with a hash of the second image.

10. The method according to claim 9, wherein the second image is a derivative of the first image.

11. The method according to claim 10, further comprising the step of storing information related to the first image in the database, wherein the information related to the first image is stored according to the hash of the first image.

12. The method according to claim 11, wherein the information related to the first image comprises at least one of metadata, location, date, permission level, security access levels, an audit trail, analyst comments, notes, files and past usage information.

13. The method according to claim 11, further comprising the step of storing information related to the second image in the database.

14. The method according to claim 13, wherein the information related to the second image is stored according to the hash of the second image.

15. The method according to claim 14, wherein the information related to the first image comprises at least one of metadata, location, date, permission level, security access levels, an audit trail, analyst comments, notes, files and past usage information.

16. A method of managing images, the images including a first image comprising a first identifier steganographically embedded therein in the form of a digital watermark and a second image comprising the first identifier steganographically embedded therein in the form of a digital watermark, said method comprising the steps of:

in a database registry, associating a first hash of the first image with a first data record associated with the first image;

in the database registry, associating a first hash of the second image with a second data record associated with the second image; and

linking the first data record and the second data record with the first digital watermark identifier.

17. A method of indexing a database managed according to the method of claim 16, said method comprising the step of:

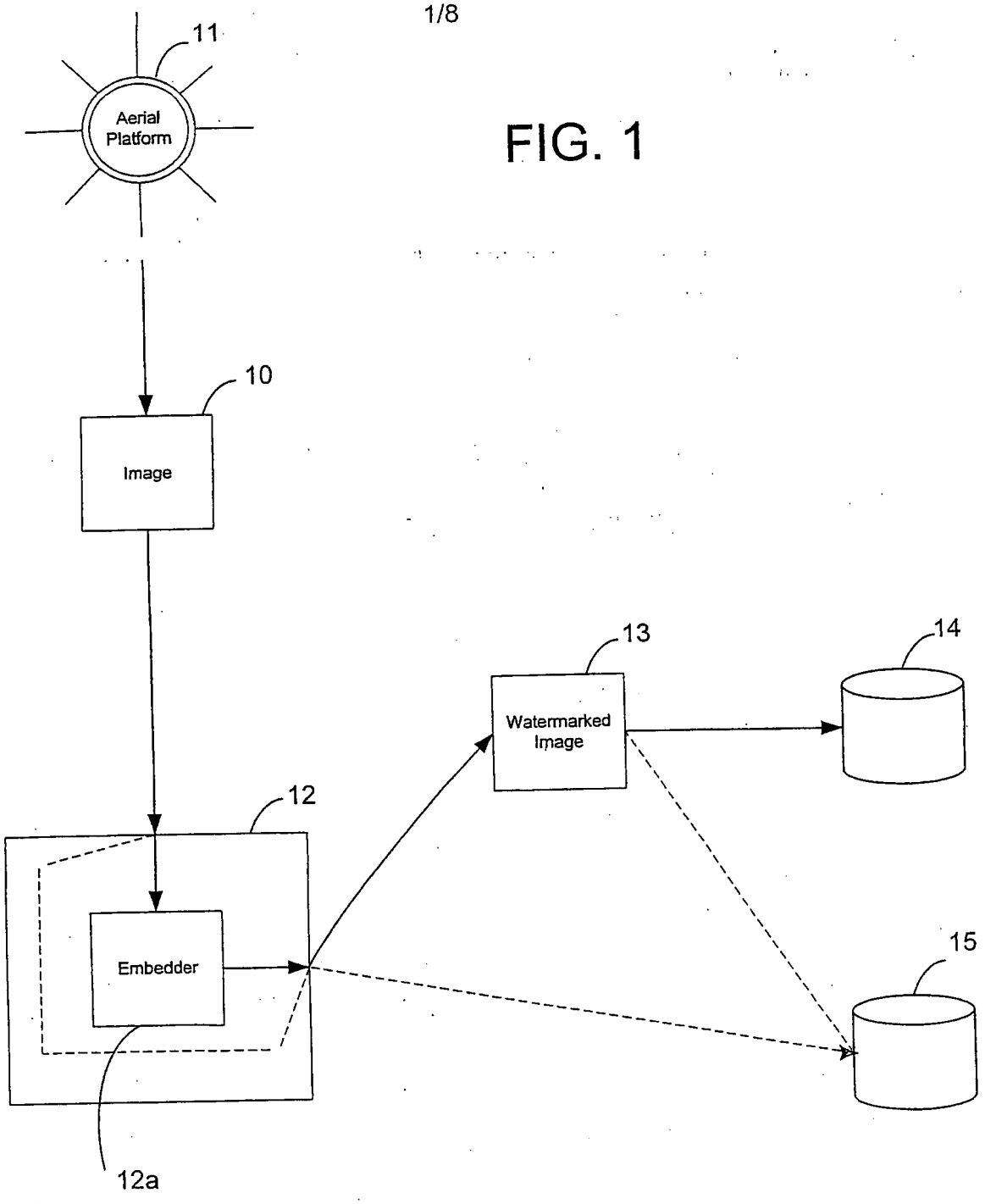
interrogating the database registry with the first hash of the first image to locate the first data record.

18. The method of claim 17, further comprising the step of accessing the second data record through the first digital watermark identifier.

19. The method of claim 17, wherein the first data record and the second data record each respectively comprise the first image and the second image.

20. The method of claim 17, wherein the second image is a derivative of the first image.

FIG. 1


11
Aerial Platform
10
Image
13
Watermarked Image
14
12
Embedder
15
12a

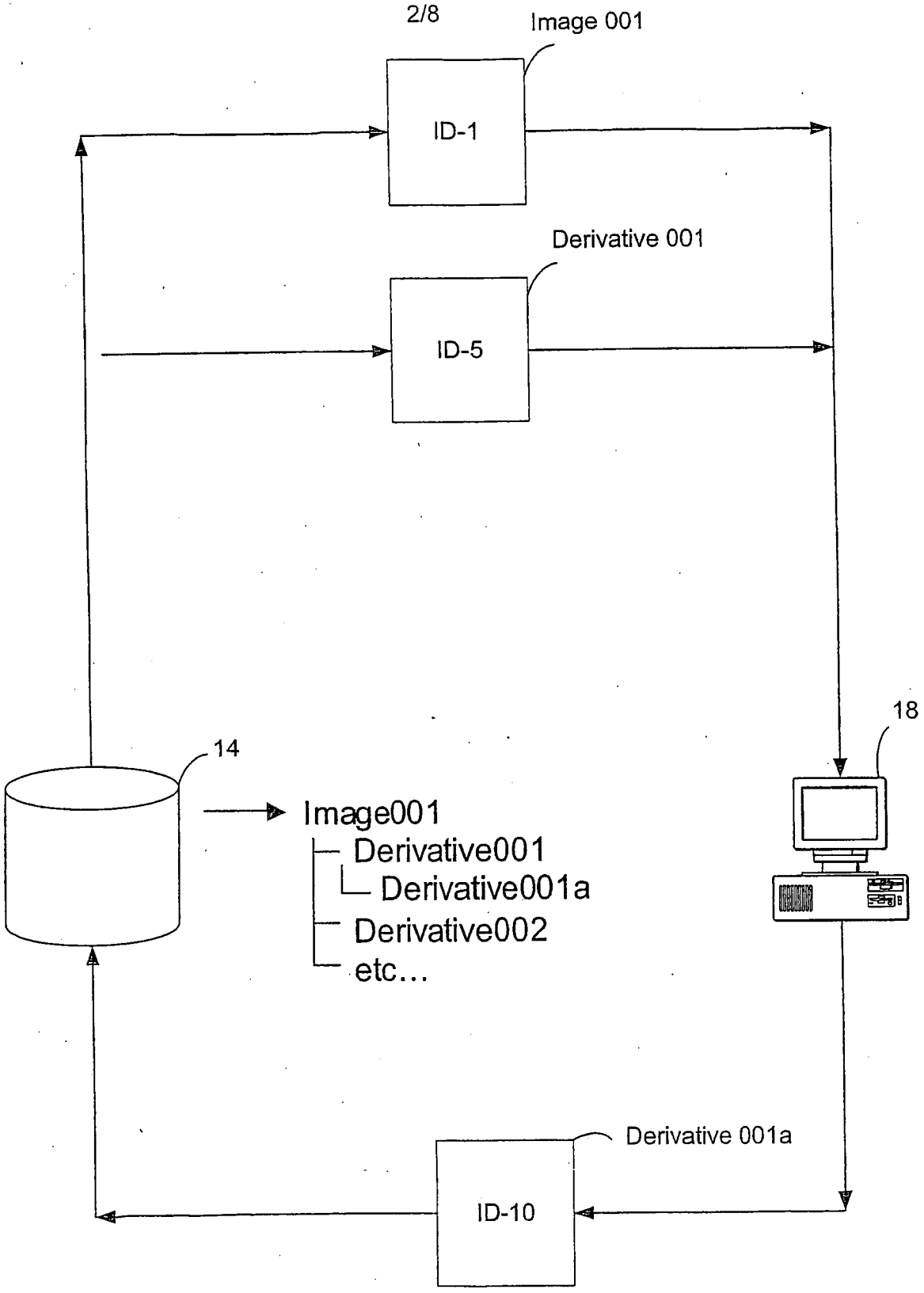


Image 001
ID-1
Derivative 001
ID-5
18
14
Image001
Derivative001
Derivative001a
Derivative002
etc...
Derivative 001a
ID-10

FIG. 2

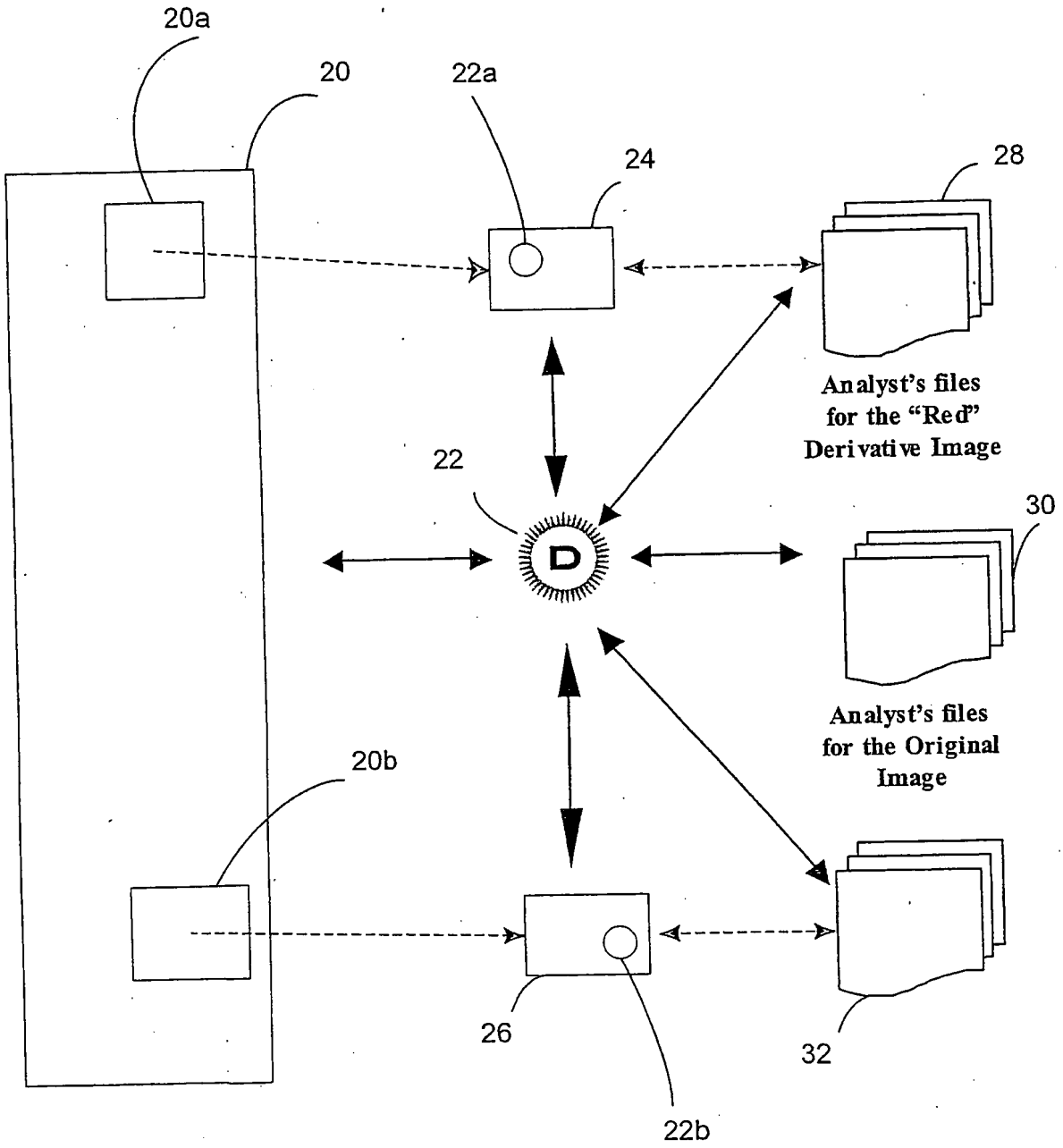

20a
20
22a
24
28
Analyst's files for the "Red" Derivative Image
22
D
30
Analyst's files for the Original Image
20b
26
32
22b

FIG. 3

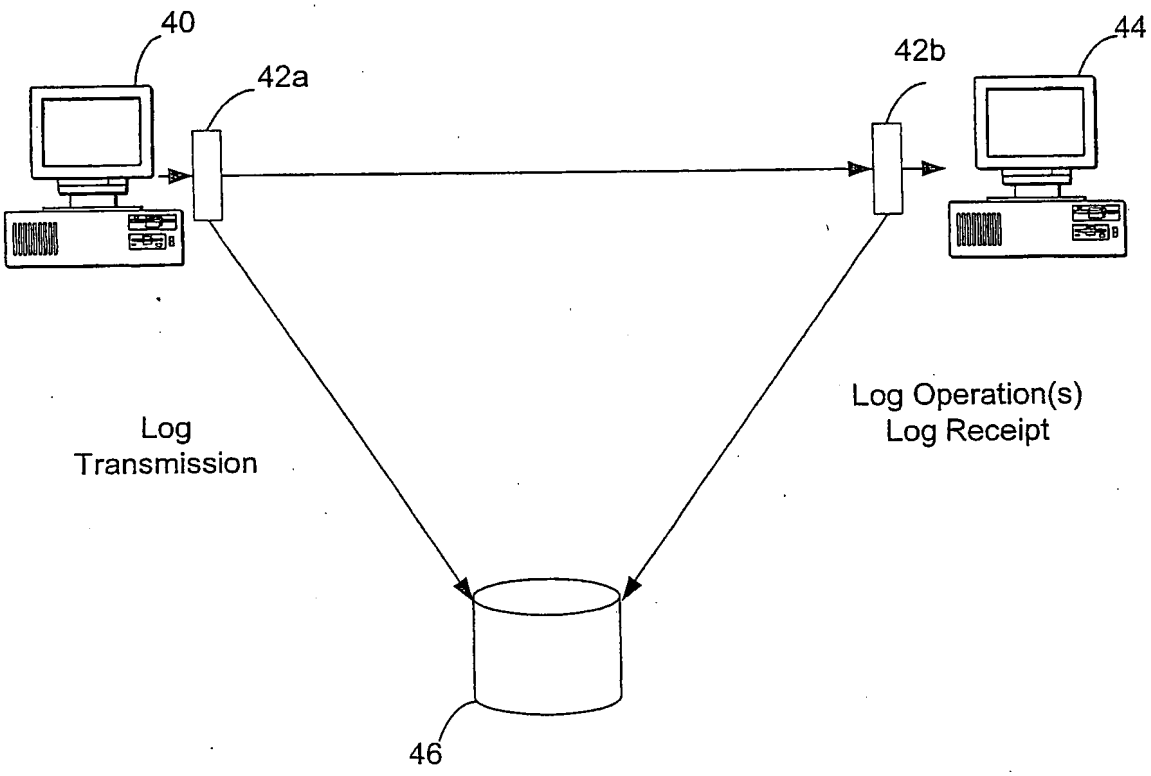

40
42a
42b
44
Log
Transmission
Log Operation(s)
Log Receipt
46

FIG. 4

FIG. 5

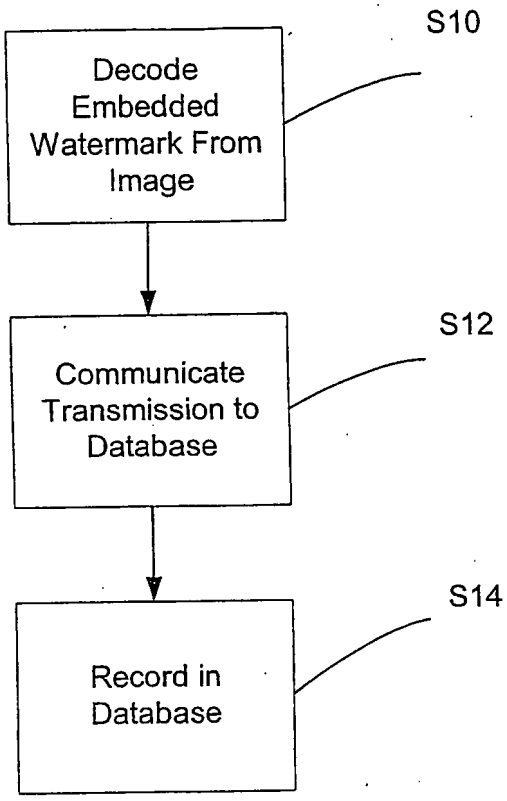
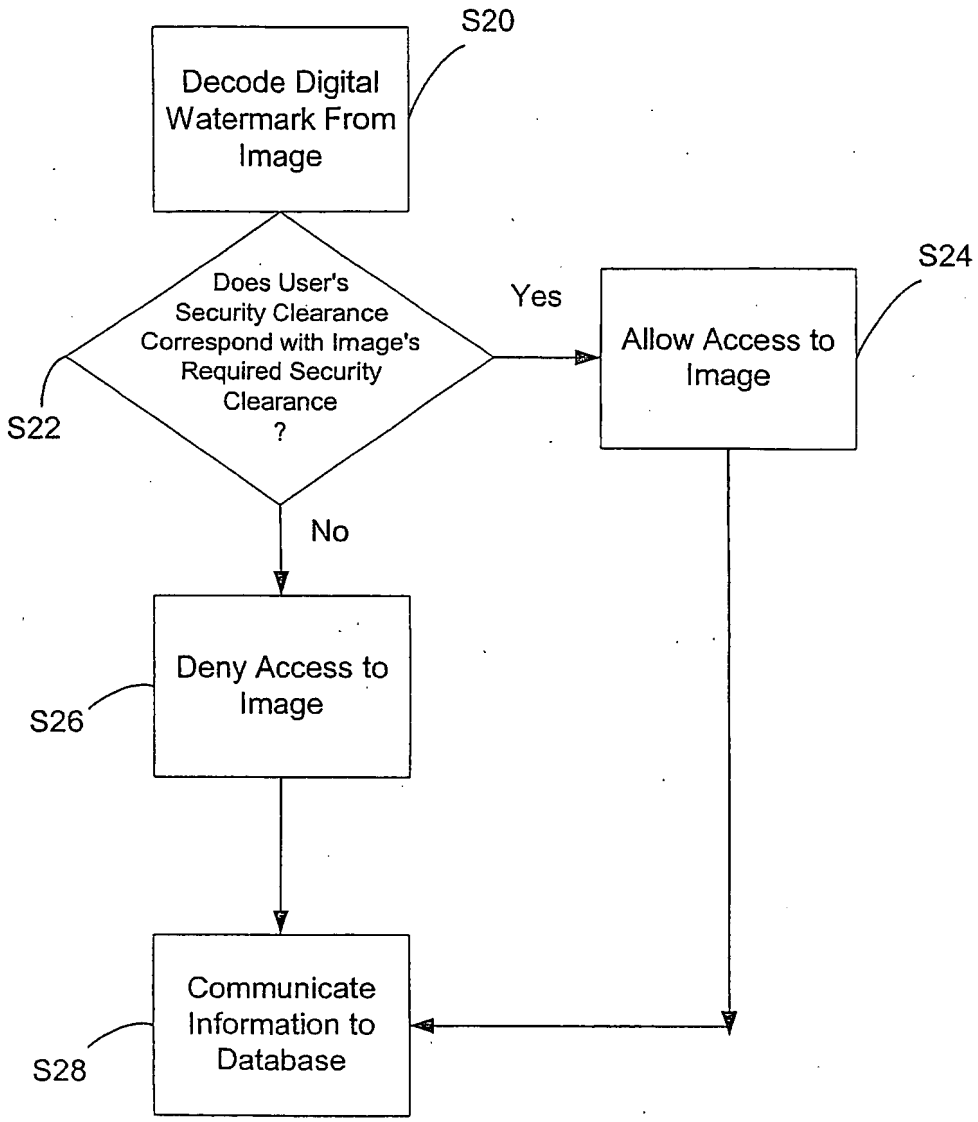

S10
Decode Embedded Watermark From Image
S12
Communicate Transmission to Database
S14
Record in Database

FIG. 6


S20
Decode Digital Watermark From Image
Does User's Security Clearance Correspond with Image's Required Security Clearance ?
S22
Yes
S24
Allow Access to Image
No
Deny Access to Image
S26
Communicate Information to Database
S28

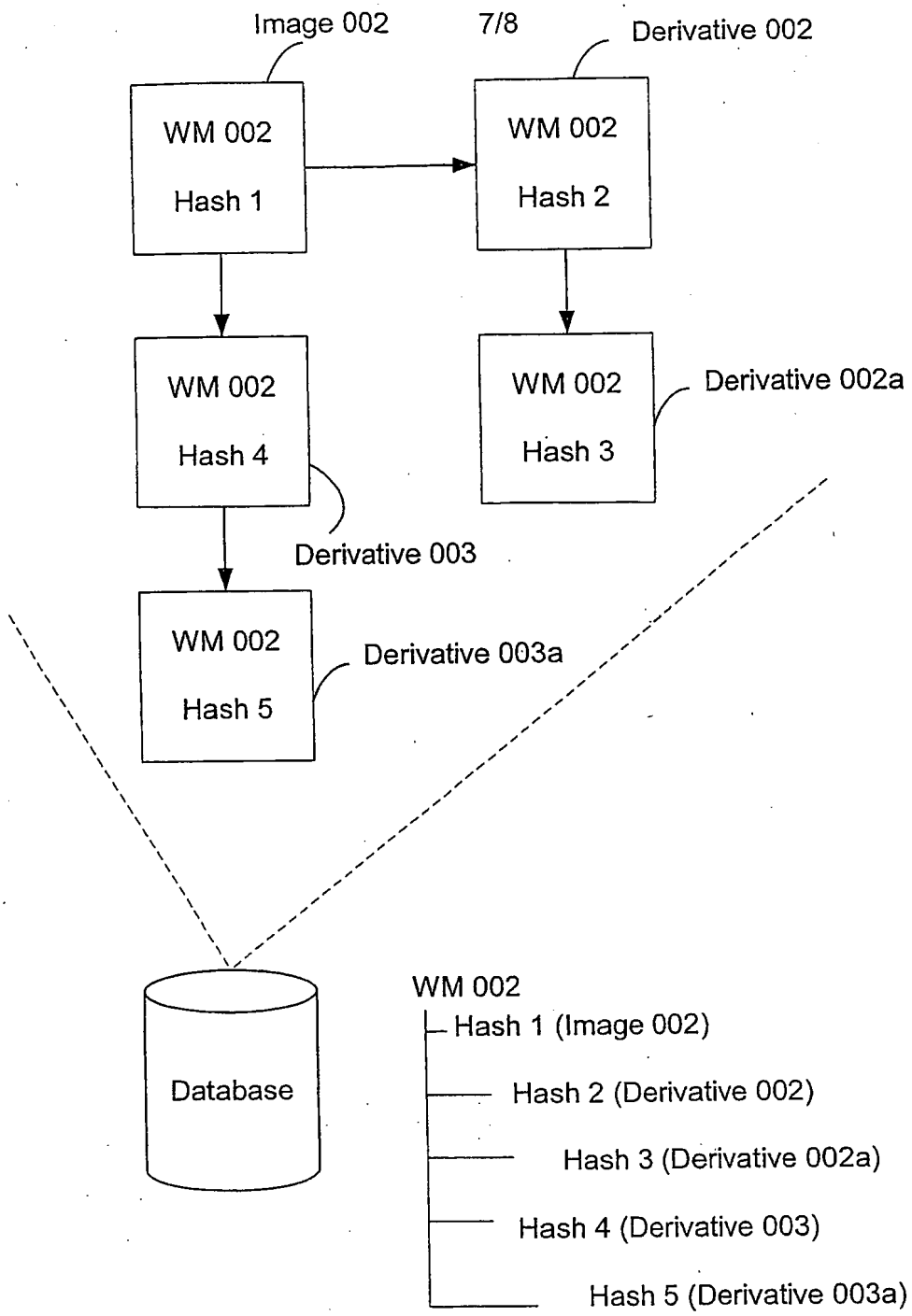
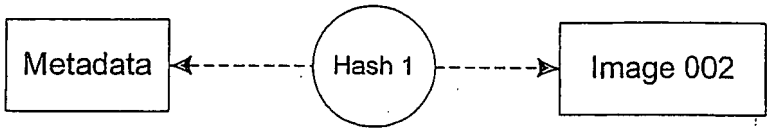


Image 002
Derivative 002
WM 002
Hash 1
WM 002
Hash 2
WM 002
Hash 4
WM 002
Hash 3
Derivative 002a
Derivative 003
WM 002
Hash 5
Derivative 003a
Database
WM 002
Hash 1 (Image 002)
Hash 2 (Derivative 002)
Hash 3 (Derivative 002a)
Hash 4 (Derivative 003)
Hash 5 (Derivative 003a)

FIG. 7

FIG. 8



INTERNATIONAL SEARCH REPORT

International application No.
PCT/US03/07776

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :H04L 9/00; G06K 9/62; H04L 9/32; H04B 1/66

US CL : 380/262; 382/100; 713/170, 176, 187; 375/240

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/262; 382/100; 713/170, 176, 187; 375/240

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EAST

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,088,394 A [MALTBY] II July, 2000, figure 3, abstract, lines 10-14, column 3, lines 59-60, column 6, line 29 to column 7, line 36	1-20

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 09 JUNE 2003	Date of mailing of the international search report 30 JUN 2003
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer ANTHONY J. BLACKMAN Telephone No. (703) - 305-3230

Form PCT/ISA/210 (second sheet) (July 1998)*